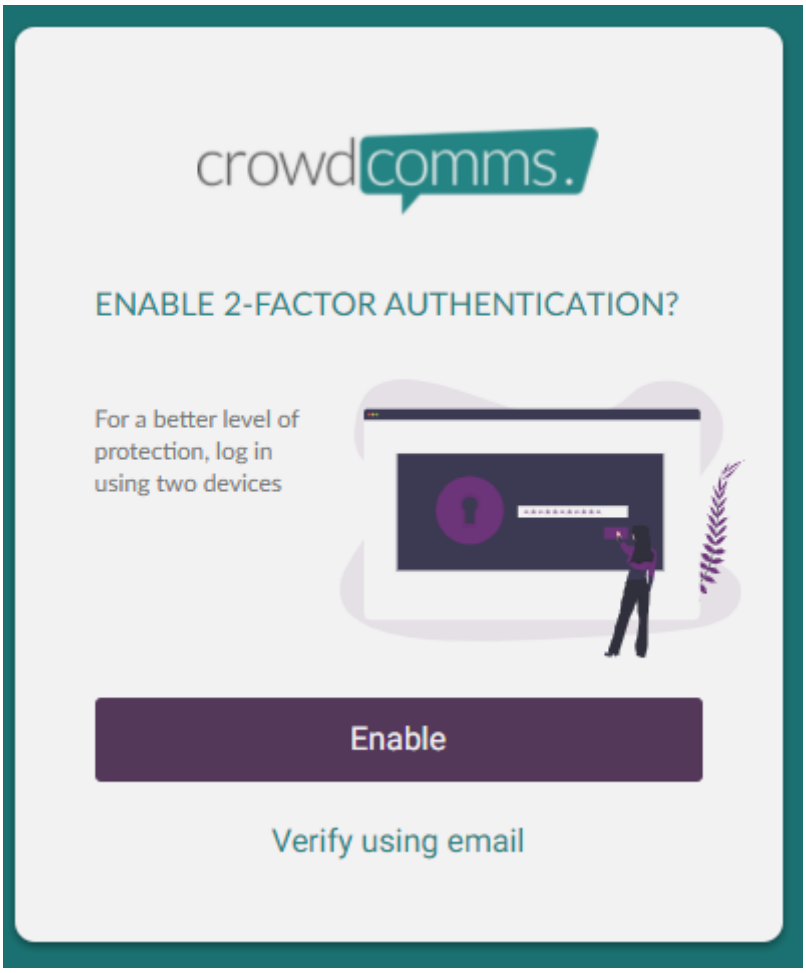
Two Factor Authentication for CMS Use

Setting Up 2FA

2FA can be enabled either by an authentication app or by getting a verification code sent to your email address.

N.B. If it is your first time accessing the CMS since the roll out of multi-factor authentication, then you may need to close your browser, re-launch and then clear your cache and cookies before accessing the CMS.

When first setting up 2FA you will be presented with this screen:



If you choose to use an authentication app then please select ‘enable’. This gives better protection as it requires the use of 2 devices. If you however would rather verify by email, you can as this is still an additional layer of security.

To set up using an authentication app:

Scan the QR code or manually enter the 16 digit code (sometimes referred to as a KEY) using your Authenticator App on your personal device

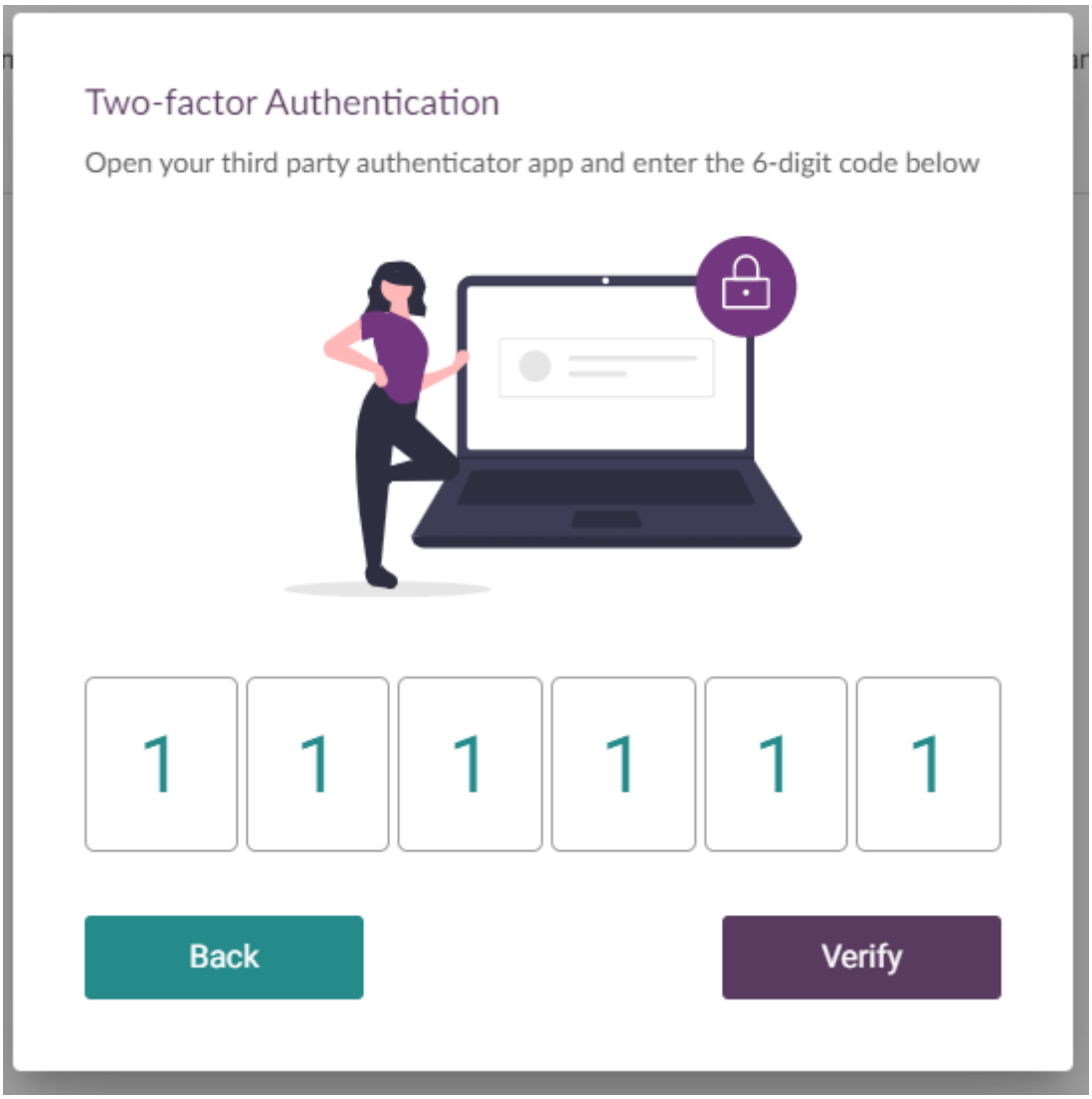
Once you have either scanned the QR code or entered the 16 digit code manually, you will then be provided with a 6 digit ONE TIME ONLY code to enter

N.B The 6 digit code is only valid for 60 seconds (Your Authenticator App will provide you with a new code after this time expires).
If you are unfamiliar with authentication apps, then here are some common ones you can use:

- *Authy*
- *Microsoft Authenticator*

- *Google Authenticator*
- *LastPass*
- *OTP*

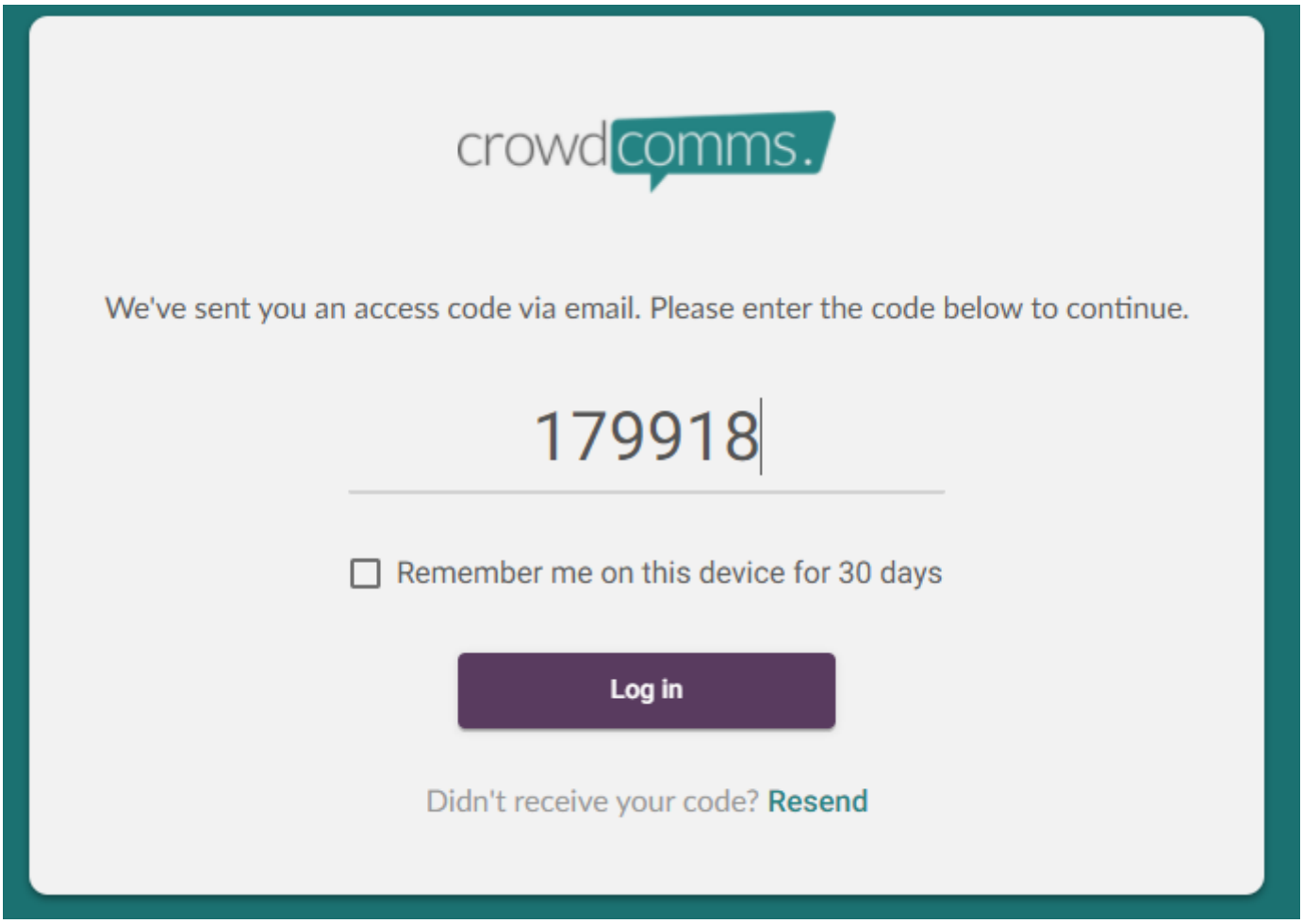
Input the 6 digit code and then click "Verify"



You will now be logged into the CMS

Email Verification

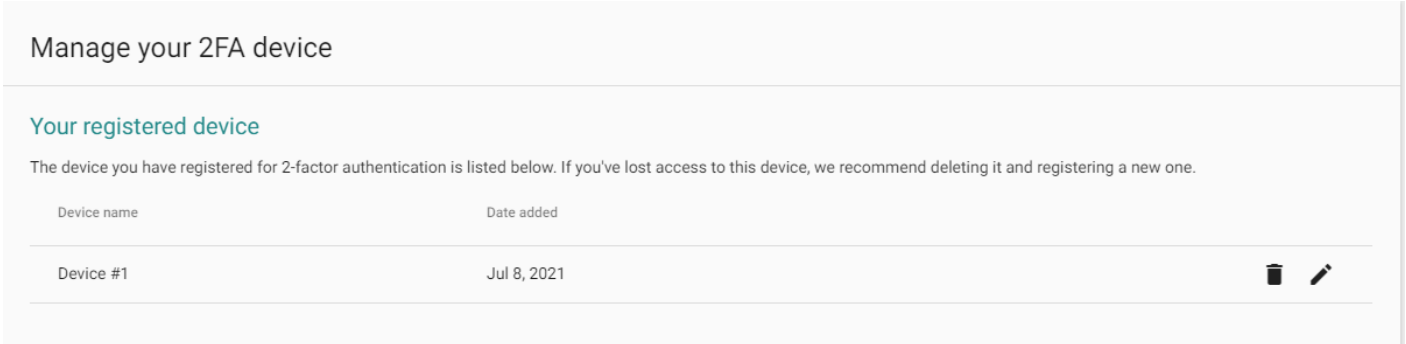
If you opt for email verification, a 6 digit code will be sent to the email address associated with your CMS account.



N.B. For both routes, you have the option to ‘trust this computer for 30 days’ to save you verifying every time if you don’t want to.

How to Manage your CMS Device

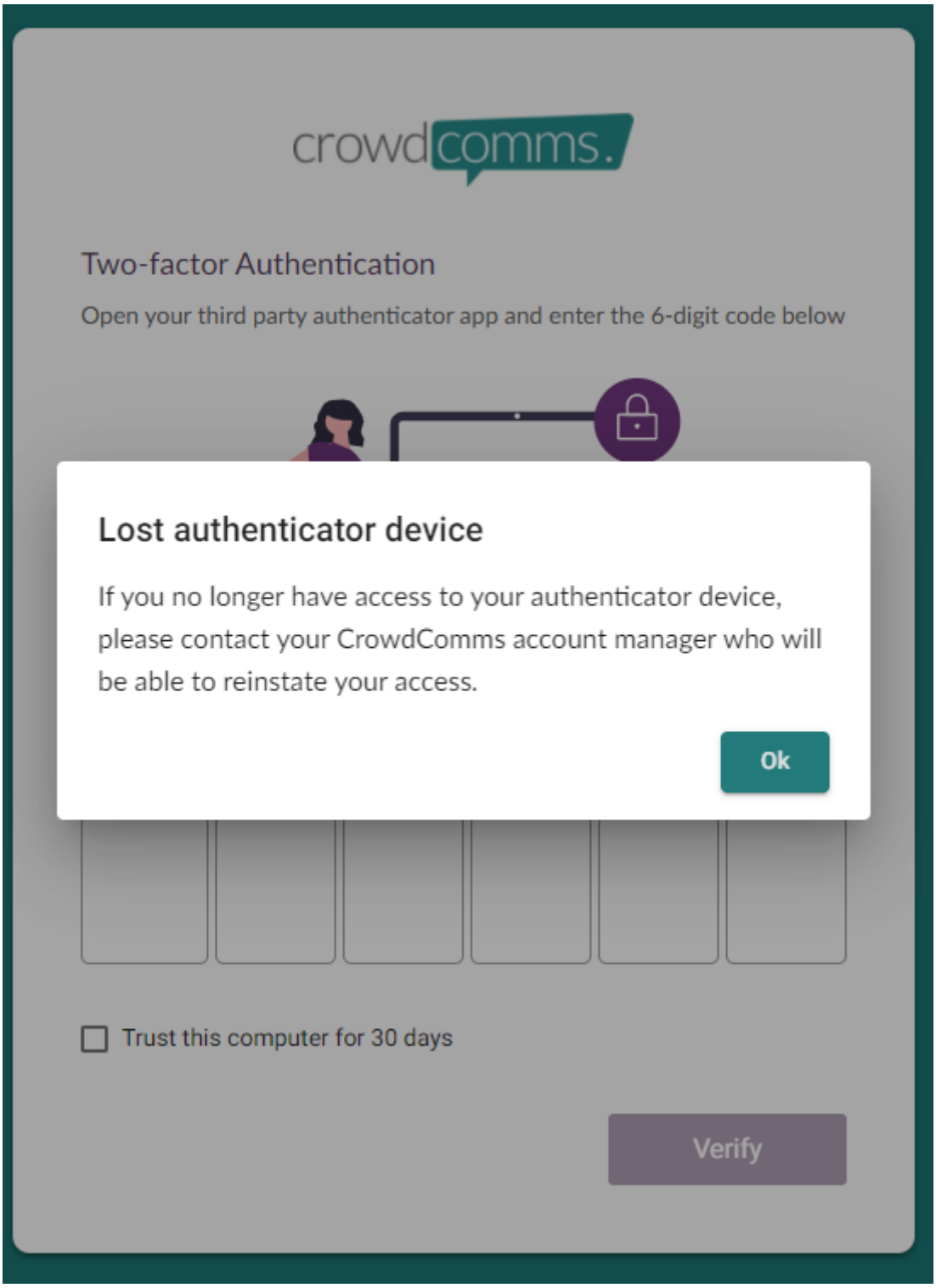
In the top-right hand profile menu you will see the option to ‘manage devices’. Here you will see a device if you chose to use an authentication app. You can click the pencil to re-name it so you know exactly what device you used if helpful.



N.B. You can only have one authentication device at a time for CMS access, so if you want to change devices, you will need to click the trash can to remove the first one. Once you have no devices, you will see the option to ‘add device’. This will then take you through the previous

process to set up 2FA.

If you lose your device, you will need to contact your designated member of our team as only CrowdComms staff can reset this for you. You will be prompted to do this by the system anyway if you select this option when trying to login. We will then reset it for you.



Revision #3
Created 8 July 2021 14:16:16 by Steven Slesser
Updated 19 August 2021 16:26:36